SMB spending on security management services worldwide will grow to almost USD35 billion by 2025

August 2021

Eileen Zimbler

USD1 out of every USD3 spent by small and medium-sized businesses (SMBs) worldwide on cyber security in 2020 was for security management services. In total, SMBs worldwide spent more than USD20 billion on remotely managed security and security product support services in 2020.[1] Analysys Mason projects that this spending will reach USD34 billion by 2025.

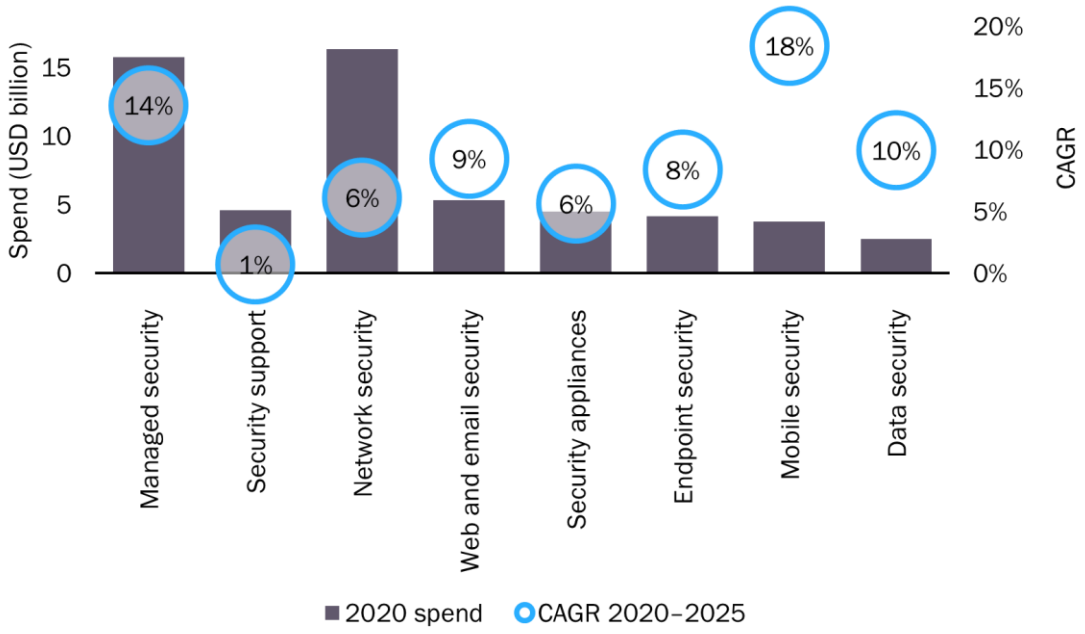
These growing levels of investment are being driven by SMBs' increasing awareness of cyber-security breaches and their consequences, as well as the rapid shift to remote working due to the COVID-19 pandemic. SMBs are being exposed to a greater number and a wider range of cyber attacks than ever before, and also have less control over who is accessing their employees' devices. All of this has highlighted SMBs' need for help with security management.

Spending on remotely managed security services accounted for 28% of SMBs' total cyber-security spend worldwide in 2020

SMBs' spending on managed security services in 2020 accounted for 28% of the total SMB spend on cyber security worldwide. This spending is expected to grow rapidly at a CAGR of 14% between 2020 to 2025 (Figure 1). 77% of SMBs' spending on security management services in 2020 was for remotely managed security services; the remainder was for security product support services.

1 Remotely managed security is the ongoing remote management of an organisation's security solutions by a third party (this includes the monitoring and management of intrusion prevention systems (IPS) and firewalls, managed detection and response (MDR) services and overseeing patch management activities). Managed security services can be provided by the vendors themselves or by their channel partners (the latter often use remote monitoring and management (RMM) tools for delivery). Security product support services include support related to the design of security systems, penetration testing, the installation of security solutions and their maintenance.

Figure 1: SMB spend on cyber security, by category, worldwide, 2020 and the associated CAGRs, 2020–2025



Source: Analysys Mason, 2021

There are several factors driving the rapid growth in SMBs' spending on remotely managed security services.

- There has been a marked increase in the number of cyber attacks since the rise of remote working, and SMBs are aware that their current security solutions may not provide adequate protection. SMBs do not always keep their solutions up-to-date or configure them properly, nor do they adapt their security policies to changes in the threat landscape.

- Many SMBs do not have access to cyber-security experts. This responsibility often falls to staff who lack security expertise.

- It is likely that large numbers of employees will continue to work remotely and access corporate networks from outside of their offices once the COVID-19 crisis has abated. SMBs should continue to deploy cyber-security solutions related to remote working, but will need external help to manage the associated complexity.

We do not believe that any of these issues will go away in the near future. Indeed, 26% of the respondents to our survey of 1870 SMBs across Australia, Canada, the UK and the USA said that at least 25% of their employees worked from home prior to the pandemic, and 44% said that at least 25% of their staff will work remotely once the crisis is over.[2]

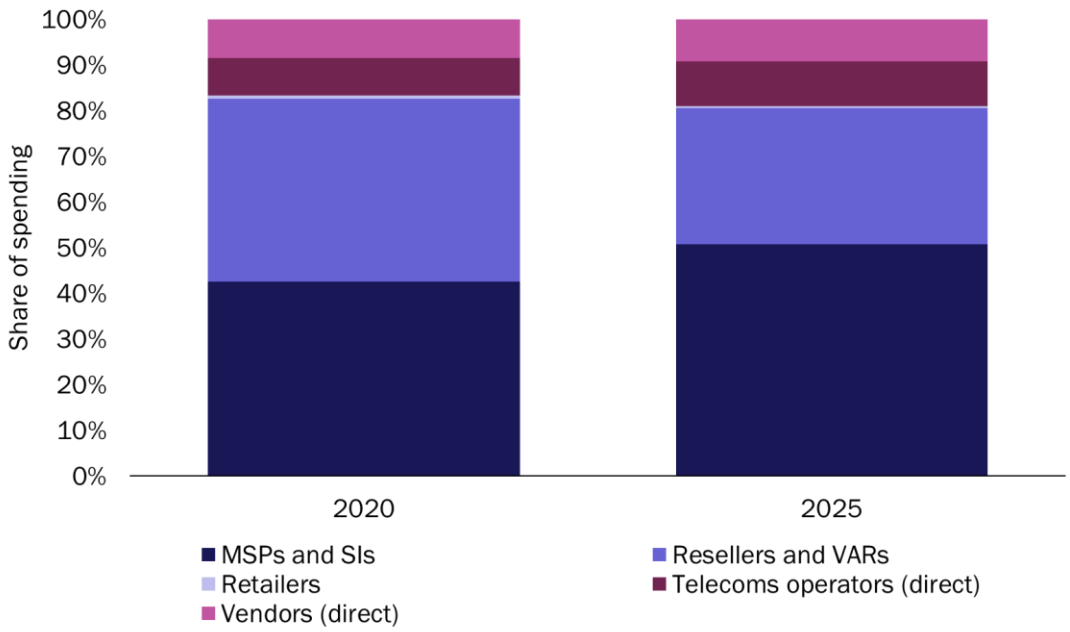
2 *Question:* "What proportion of your employees worked from home regularly prior to the start of the COVID-19 pandemic and what proportion do you expect to work from home once the crisis is over?"; *n* = 1870.

We also asked SMBs about their planned spending on cyber security and managed services. 88% of SMBs estimated that their spending on cyber-security solutions in 2021 will be higher than or the same as their spending in 2020;[3] 85% said the same about their spending on managed services.[4]

SMBs lack the internal resources to adequately protect their data assets and are turning to MSPs for help

SMBs' spending on security management services is shifting from resellers and value-added resellers (VARs) to managed service providers (MSPs), system integrators (SIs) and telecoms operators.[5] Indeed, SMBs spent USD10 billion on security management services with MSPs, SIs and operators in 2020 (51% of SMBs' total security services), but we expect that this will increase to USD21 billion by 2025 (61% of the total) (Figure 2).

Figure 2: Share of SMB spending on security management services, by route to market, worldwide, 2020 and 2025[6]



Source: Analysys Mason, 2021

This migration is not surprising. Most SMBs lack the internal resources to adequately protect their data assets, and it is easier to employ an MSP than hire more staff (and often cheaper). The COVID-19 crisis has accelerated SMBs' shift to working with MSPs due to the increase in remote working, so it makes more sense than ever for SMBs to have an MSP partner rather than having an internal IT team or an outside IT consultant on-premises. Many resellers and VARs are actually transforming into MSPs as they adapt to changes in businesses' requirements.

3 *Question:* "Please tell us about your company's anticipated 2021 [cyber security (e.g., endpoint/anti-virus, anti-malware, web/messaging security, cloud security, etc.)] spending compared to your actual spending in 2020?"; *n* = 1870.

4 *Question:* "Please tell us about your company's anticipated 2021 [managed services (e.g., remotely or cloud-managed networking/Wi-Fi, or managed PCs, etc.)] spending compared to your actual spending in 2020?"; *n* = 1870.

5 Analysys Mason's definition of MSPs includes managed security services providers (MSSPs).

6 Note that the chart represents the spending within the channel that sells the product/service to the business. If a vendor sells a product through an MSP, this sale is captured under 'MSPs and SIs'. If a security product is supplied by a telecoms operator, but sold by a reseller, this sale is captured in the 'resellers and VARs' category.

Security vendors need to develop stronger partnerships with MSPs, SIs and telecoms operators

SMBs are increasingly trusting MSPs with their technology decisions, and security vendors have been taking notice. Indeed, many vendors are developing and upgrading their solutions, incentive programmes and management portals for MSPs. Vendors must make it clear how their products make it easier and more profitable for MSPs to address SMBs' security needs in order to succeed.

Security vendors should also develop stronger partnerships with telecoms operators because they can broaden their exposure to the SMB space. Operators tend to have strong existing relationships with numerous SMB customers, and many SMBs are often willing to take adjacent services from operators, such as firewalls, DDoS protection or endpoint security. Vendors are not taking advantage of this relationship as much as they could. Some operators are working to upgrade their in-house cyber-security management competences, while others are acquiring third-party managed security providers. Vodafone is partnering with systems integrator Accenture to help it to deliver managed security services to SMBs.

Several operators are working on becoming "trusted advisors" to their SMB customers. Companies such as BT, Singtel and Vodafone are all promoting SMB-focused programmes that aim to improve SMBs' digital transformation and educate SMBs on a variety of topics, including cyber security. Vendors should take advantage of operators' expanding cyber-security advisory role.